PRIVACY 102
TRAINING FOR SUPERVISORS

PRIVACY ACT OF 1974

5 U.S.C.552a

PRIVACY TOOL BOX

- WEB SITE: WWW.PRIVACY.NAVY.MIL

  - **Lists all approved Navy and Marine Corps Privacy Act systems of records**
  - **DOD systems and Government-wide systems**
  - **SECNAVINST 5211.5E, DON Privacy Program**
  - **Provides guidance**
  - **Contains training packages**
  - **And so much more!**

PRIVACY REFRESHER

- From Privacy 101, you know that the Privacy Act is…
  - **A means to regulate the collection, use, and safeguarding of personal data**
  - **A statute that only applies to the Executive Branch of the Federal Government**

PRIVACY REFRESHER

- **In Privacy 101, you also learned that the Privacy Act**
  - **Only applies to U.S. Citizens and those individuals who have been admitted for permanent legal residence**
  - **Covers “systems of records” – A group of files that**
    - **Contains a personal identifier**
    - **Contains one other element of personal data**
    - **Is retrieved by personal identifier**

PRIVACY REFRESHER

- Privacy provides citizens and lawful aliens with guaranteed rights to:
  - **Access/amend their records, ensuring they are accurate, timely, and complete**
  - **To appeal agency decisions**
  - **To sue for breaches**

PRIVACY REFRESHER

- Privacy 101 also taught you that:
  - **Agencies may not collect personal data without first publishing a system notice in the Federal Register that announces the collection**
  - **The system notice sets the rules for collecting, using, storing, sharing, and safeguarding personal data**

AS A SUPERVISOR…

- **You and your staff**
  - **May initiate data collections**
  - **Receive privacy data in the course of conducting business**
  - **Create, manage, or oversee files or databases containing personal data**
  - **And, disseminate personal data**

ACCORDINGLY, YOU HAVE A DUTY TO ENSURE THAT…

- **Your staff receives Privacy Act training**
- **They abide by Privacy Act protocols when collecting, maintaining, destroying, or disseminating personal information**
- **They safeguard personal information**
- **They identify what PA systems notice allows the collection and follows the rulemaking set forth in the notice**

REVIEW YOUR OFFICE PROTOCOLS

- **What databases are your maintaining that contain personal information?**
  - **Can you identify the Privacy Act systems notice that permits the collection?**
  - **Are you properly safeguarding those records?**
  - **Are you properly disposing of those records?**
  - **Are you properly marking those records when they are being transmitted?**
  - **Are you posting those documents on the internet? Intranet? Public folder?**

REVIEW YOUR OFFICE PROTOCOLS

- **Are you only sharing those records with individuals who have an official need to know?**

- **Are you following proper records management practices for maintaining, accessioning, or destroying those records?**

DO YOU DIRECTLY SOLICIT PERSONAL DATA?

- If yes, does the form contain a Privacy Act statement? Is that statement up-to-date?

- What system of records allows the collection?

- What safeguards do you have in place to prevent inadvertent disclosure?

REMEMBER, YOU CAN NOT…

- Initiate new collections of personal data
- Add new elements to an existing and approved data base
- Create or revise forms that collect personal data
- And/or deploy surveys

Without thinking P-R-I-V-A-C-Y !

ACCESS TO PERSONAL INFORMATION

- **Do you and your staff practice limited access principles?**
  - **Grant access to only those specific employees who require the record to perform specific assigned duties**
  - **You and your staff must closely question other individuals who ask for your data**
    - **Why do they need it? How will it be used?**
    - **Is the purpose compatible with the original purpose of the collection?**

TRANSMITTING PERSONAL DATA

- **Do not use interoffice mail envelopes to route personal data-use sealable envelopes addressed to the authorized recipient**

- **Properly mark personal data that you transmit via letter or email: “For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties”**

SAFEGUARD PERSONAL DATA

- **Store in an out-of-sight location**
- **Do not leave out in open spaces**
- **Take steps to properly destroy data to preclude identity theft**
- **Only share with individuals having an official need to know**
- **Do not lose control of the record**

MAKE PRIVACY A PRIORITY

- Voice your commitment to protecting personal privacy
- Share the DON Code of Fair Information principles with your staff
- Remind staff to use caution when posting data to shared drives, multi-access calendars, etc

MAKE PRIVACY A PRIORITY

- **Periodically review shared devices for compliance**
- **If you have a web site, ensure that documents posted therein do not contain personal data**
- **As you move from paper to electronic records, review established practices to determine if they are best practices**
- **Don’t collect personal data because you might need it – collect it because you do need it – what you collect you must protect!**

IF YOU HAVE CONTRACTORS

- **Ensure they understand Privacy and comply with all Privacy protocols**
- **Ensure that the contract includes the federal acquisition regulation Privacy clauses in the contract (far 52-224-1 & 52.224-2)**
- **Ensure language in the contract addresses how data is to be disposed at the end of the contract**

RECALL ROSTERS

- Yes you may have a recall roster

- The collection is permitted by PA systems notice NM05000-2, Administrative Personnel Management System

SOLICITING INFORMATION FOR A RECALL ROSTER

- **Civilian employees and contractors are encouraged to give supervisors their home telephone numbers, but do not have to agree to share them with co-workers**

- **If an employee objects to having his/her telephone number placed on a recall roster:**
  - **List “unlisted” or “unpublished” instead of the home number**
  - **Arrange to call the employee yourself during alerts or exercises**

SOLICITING INFORMATION FOR A RECALL ROSTER

- **Properly mark the recall roster "For Official Use Only – Privacy Sensitive: Any misuse or unauthorized disclosure may result in both civil and criminal penalties."**

- **Instruct your staff that the roster is to be used for official purposes only and kept in a secure location**

WHEN PERSONAL DATA IS LOST, STOLEN, OR COMPROMISED…

- **DON seeks to ensure that all personal information is properly protected to preclude identity theft**

- **DEPSECDEF issued a memo on 15 JUL 2005 requiring DOD activities to notify affected individuals within 10 days**
- **Individuals include:**
  - **Military members and retirees**
  - **Civilian employees (appropriated and non-appropriated)**
  - **Family members of a covered individual**
  - **Other individuals affiliated with DOD/DON (e.g., Volunteers)**

WHEN PERSONAL DATA IS LOST, STOLEN, OR COMPROMISED…

- **Can’t notify the individual within 10 days?**
  - **Notify CNO (DNS-36) immediately**
  - **Include reason for delay (e.g., Notification delay at request for law enforcement authorities)**
- **In the case of multiple or unidentifiable individuals involved**
  - **Provide generalized notice to potentially affected population**

TAKE STEPS TO AVOID PRIVACY CRIMINAL PENALTIES

- **What Privacy violations may lead to criminal penalties?**
  - **Collecting data without meeting the Federal Register publication requirement**
  - **Sharing data with unauthorized individuals**
  - **Acting under false pretenses**
  - **Facilitating those acting under false pretenses**
- **Penalties:**
  - **Misdemeanor charge (jail time of up to one year)**
  - **Fines of up to $5,000**

TAKE STEPS TO PRECLUDE PRIVACY CIVIL PENALTIES

- **What Privacy violations may lead to civil penalties?**
  - **Unlawfully refusing to amend a record or grant access**
  - **Failure to maintain accurate, relevant, timely, and complete data**
  - **Failure to comply with any Privacy Act provision or agency rule that results in an adverse effect**

- **What Privacy violations may lead to civil penalties?**
  - **Actual damages**
  - **Attorney fees**
  - **Removal from employment**

PRIVACY CONSIDERATIONS

- **Most DON PA systems of records are releasable to the subject of the file in their entirety**
- **Because there is no Privacy exemption under the Privacy Act – avoid commingling information on others in the same file**
- **There is no exemption available to protect personal opinions**

SIDEBAR: Supervisor's Notes

- **If you maintain information on your employee as a memory jogger to rate their performance, are not required to maintain it, do not share it, do not file it in official files, and destroy it at your convenience – your notes do not qualify as an agency record and is not subject to access by the employee**

SIDEBAR – Supervisor's Notes

- On the other hand, if you are taking notes for the purpose of intended/possible action against an employee, they are agency records. Such records usually fall into an OPM Gov't system which makes the information releasable to the employee in their entirety.

SIDEBAR – CIVILIAN AND MILITARY PERSONNEL RECORDS

- **Both records are Privacy Act systems of records**
  - **OPM governs most civilian personnel records**
  - **N01070-3 is the PA systems notice for Navy Military Personnel Records**
  - **MMN0006 is the PA systems notice for Marine Corps Military Personnel Records**

The individual to whom these records pertain get the entire record, without exemption

SIDE BAR - LEAVE

- The type of leave a person takes is generally personal to them. Accordingly avoid listing the type of leave on a calendar, listing, check-in/out board, etc

SIDE BAR – Employee Information

- As a supervisor, do not share personal information about an employee, unless he/she has authorized you to do so
- Avoid using email to discuss personal information about an employee, as this places the information at greater risk of being compromised
- Remember, LOOSE LIPS SINK SHIPS!

FINALLY…

- **You and your staff are entrusted with personal information of others. You are the first line of defense in ensuring safeguarding privacy and protecting DON from damaging lawsuits.**

- **FACTOR PRIVACY IN YOUR WORKPLACE!!!**

- **Questions may be addressed to your local Privacy Officer or to Doris Lama, CNO (DNS-36), 202-685-6545, doris.lama@navy.mil**